

Prepared for Review and Comment by:

**National Archives and Records Administration,
Office of Management and Budget, and the Department of Justice**

Records Management Guidance For PKI-Unique Administrative Records

Deliverable: 07

Third Draft

Comments Due By: September 23, 2002

August 14, 2002

Task Order 02: Federal PKI Infrastructure Records Management Guidance Support

Contracting Officer: Frank Rumph, Tel. 703/306-4505

Contracting Officer's Technical Representative: Ann Townsend, Tel. (703) 308-6846
Fax (703) 308-6879

Government Task Manager: Mark Clayburn, (703) 305-8577

Government Technical Managers: Mark Giguere, (301) 713-7110 x250, FAX (301) 713-6852
Arthur F. Purcell, (703) 308-6868, FAX (703) 308-6916

Prepared by:
COHASSET ASSOCIATES, INC.
Charles Dollar and Richard Fisher

Table of Contents

DOCUMENT STATUS	1
1. INTRODUCTION	2
2. BACKGROUND.....	4
3. PURPOSE AND SCOPE	6
4. PKI RECORDS PRODUCING FUNCTIONS AND ACTIVITIES	9
5. PKI-UNIQUE RECORDS MANAGEMENT GUIDANCE.....	14
5.1 GUIDANCE FOR OPERATIONAL SYSTEMS.....	16
5.2 GUIDANCE FOR RECORDKEEPING SYSTEMS.....	23
APPENDIX A. GLOSSARY, ACRONYMS AND ABBREVIATIONS	30
APPENDIX B. EXAMPLE PKI-UNIQUE ADMINISTRATIVE RECORDS SERIES	35
APPENDIX C. FOCUS GROUP ISSUES.....	40

Document Status

This Third Draft of the Records Management Guidance for PKI-Unique Administrative Records has been produced for review by the National Archives and Records Administration (NARA), Office of Management and Budget (OMB) and the Department of Justice (DOJ). It addresses the comments received from the Federal PKI Steering Committee's review of the Second Draft.

Comments and suggestions for this Third Draft are requested by Monday, September 23, 2002. Of particular importance for review and comment are the detailed guidance identified in Section 5. PKI-Unique Records Management Guidance, and the examples of PKI administrative activities and records presented in Section 4. PKI Records Producing Functions and Activities.

1. Introduction

A public key infrastructure (PKI) is defined as “a set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.”¹ A PKI also is an asymmetric cryptography security environment that is built on a set of standards and guidelines that require the production, receipt, and maintenance of certain administrative records during the planning, implementation, operation, auditing/monitoring and reorganization or termination of the infrastructure.

Regulatory, legal or audit issues could arise during the operation of PKIs in the conduct of business by federal agencies that require the retrieval and delivery of administrative PKI records, and may also be required in the course of subsequent agency business transactions. Therefore, retaining and managing records according to regulations and good practices for the authorized retention period should be fundamental elements of a PKI. With the understanding that a record file copy is established as soon as data content or document content is finalized or received, this fundamental need for records management as an integral part of a PKI and applies whether the records are being retained and managed in an operational system², or in a recordkeeping system³.

As a means to assist agencies in the management of PKI administrative records, the development of this guidance was jointly initiated by NARA and the Legal and Policy Working Group [L/P WG] of the Federal Public Key Infrastructure Steering Committee [FPKISC], which operates under the mandate of the Chief Information Officers’ [CIO] Council.

The target audience for this guidance includes federal agency information technology, records management and operations personnel responsible for planning, implementing, operating or otherwise documenting and managing records produced by PKI administrative activities. Other entities, such as state and local government agencies, as well as commercial entities interacting with government agencies may find this guidance document useful and may adopt and or modify it to suit their specific needs.

The remaining content of this guidance is organized as follows:

Section 2. Background, discusses the situation with respect to existing records management guidance and defines specific questions that need to be answered when developing guidance unique to a PKI.

¹ *Introduction to Public Key Technology and the Federal PKI Infrastructure*, 26 February 2001, National Institute of Standards and Technology

² The software and hardware system that performs the day-to-day activities of running and maintaining a PKI, such as a CA (see Appendix A).

³ A manual or automated system in which records are collected, organized, and categorized to facilitate their preservation, retrieval, use, and disposition for the authorized retention period (see Appendix A).

Section 3. Purpose and Scope, presents the key considerations that form the basis for the records management guidance.

Section 4. PKI Records Producing Functions and Activities, describes the various processes and activities, including example records inherent in a PKI environment and categorizes them as either PKI-unique or PKI-supporting.

Section 5. PKI-Unique Records Management Guidance, delineates the guidance for the management of administrative PKI-unique records that is separated into two areas: “operational” and “recordkeeping” systems.

There are three supporting appendices: Appendix A – Glossary, Acronyms and Abbreviations; Appendix B – Example PKI Administrative Records Series, presents an example of how PKI-unique records can be logically categorized by activity; and Appendix C – Focus Group Issues, provides responses and references regarding how issues identified in the focus groups are addressed in this guidance.

2. Background

Currently, there are several general sources of guidance for managing records generated in an electronic application environment. NARA issued general records management guidance for electronic signature technologies on October 18, 2000 entitled "Records Management Guidance for Agencies Implementing Electronic Signature Technologies." NARA also has promulgated regulations in 36 CFR that provide general guidance for the management of electronic records. The Department of Defense (DoD) 5015.2 Design Criteria Standard for Electronic Records Management Software Applications delineates comprehensive guidance for the management of electronic records in general. OMB Circular A-130 contains general guidance in Appendix III related to the need for the management of records created in a security infrastructure. However, this guidance does not specifically address the management of records unique to a PKI.

Current guidance that addresses PKI-specific records is at a very high level (CARAT⁴) or only provides discussion of issues (PAG⁵), rather than setting forth specific requirements. Section 4.5.5 Records Archival of the X.509 Certificate Policy and Certificate Practices Framework (RFC 2527) dated January 3, 2002 (X.509 CP/CPS Framework), only suggests a framework for managing records and appears to relate exclusively to an operational system environment. This framework does not provide specific guidance for managing records during the authorized retention period, nor does it address the management of other PKI administrative records that are created outside of the operational system, such as a Certificate Policy (CP), Certification Practice Statement (CPS), or subscriber agreement.

Statements made in Section 4.6 Records Archival (now Section 4.5.5 of the latest X.509 CP/CPS Framework) and in several certificate policy drafts, such as the Federal Bridge Certification Authority (FBCA), Digital Signature Trust (now part of Identrus) and VeriSign, suggest that government agencies and PKI software vendors primarily are interpreting the term "records archival" as meaning "backup" of the records in a PKI operational system. This interpretation does not reflect the meaning of "archival" and "archiving" as understood by records managers: a trustworthy logical or physical repository of records that is protected from loss, alteration, and deterioration for the full duration of the authorized retention period. Satisfying various requirements for protecting records as trustworthy evidence means that they should be managed in an environment that supports the functionality required of a recordkeeping system.

In essence, the current guidance and framework are either too general or too narrowly focused to address the specific requirements for managing PKI-unique administrative records, particularly regarding higher level certificate environments where retention periods can run from ten to twenty-plus years. Examples of key questions left unanswered by current guidance are:

⁴ *CARAT Guidelines for Constructing Policies Governing the Use of Identity-Based Public Key Certificates*; National Automated Clearing House Association (NACHA), The Internet Council Certification Authority Rating and Trust (CARAT) Task Force, January 14, 2000

⁵ *PKI Assessment Guidelines (PAG)*, v0.30, Information Security Committee, Section of Science and Technology, American Bar Association, June 18, 2001

- Since the X.509 CP/CPS Framework, Section 4.5.5 Records Archival appears to focus on operational PKI systems, what guidance is needed to manage records that are created or received outside of the operational system, such as paper records or records created and stored in electronic form by an office productivity application?
- If the data that underlies records are being retained in database tables on the operational system and also being retained as the record file copy for the full retention period, what is needed on the operational system to manage the disposition of the records according to the authorized retention schedule?
- What data elements (metadata) should be available on the operational system to allow for either:
 - Managing the disposition of database records when the authorized retention period expires?
 - Transferring database records to a recordkeeping system for management during longer term retention periods?
- Should non-current or non-active PKI-unique records (e.g., expired digital certificates) be transferred from an operational system to a recordkeeping system and, if so, when and using what methods?
- If records are transferred from an operational system to a recordkeeping system, what practices should be in place to ensure a complete and accurate transfer?
- If the record file copy is maintained in a recordkeeping system, what practices need to be followed to preserve it for a long term retention period (10-20 years)?

This guidance document is aimed at providing answers to these questions in the form of perspectives, examples and guidance for managing PKI administrative records.

In an effort to determine the areas and issues that should be considered when developing more detailed PKI administrative records management guidance, two Focus Groups sessions with participants from multiple federal agencies were conducted on March 18 and 20, 2002. Key issues identified in these Focus Groups are presented and discussed in Appendix C. and have been addressed, as appropriate, in Section 5. PKI-unique Records Management Guidance.

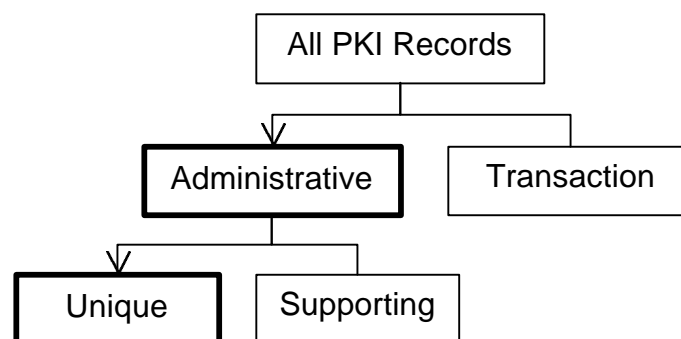
3. Purpose and Scope

This document provides records management guidance for both operational and recordkeeping environments that will assist federal agencies in the management of administrative records produced or received during the planning, implementation, operation, audit or monitoring and reorganization or termination of a PKI. This guidance supplements the general electronic signature records management guidance issued by NARA on October 18, 2000 entitled "Records Management Guidance for Agencies Implementing Electronic Signature Technologies."

The focus of this guidance is on PKI-unique administrative records (as opposed to transaction records that incorporate the use of a public key certificate or cryptographic key). PKI-unique records are specific to the administrative functions related to planning, implementing, operating, auditing or monitoring, and reorganizing or terminating a PKI. Records that are not unique to a PKI are called "supporting records." Supporting records are data or documents that are produced in most implementations of a computer or communications security infrastructure and are covered by existing records schedules or other guidance. Examples of supporting records are hardware/software documentation, training records, and personnel records (which are specifically covered in a General Records Schedule). While this document identifies both the unique and supporting functions and activities that are part of a PKI, this guidance focuses specifically on records that are unique to the PKI.

The following diagram delineates the specific group of records, namely PKI-unique records (in the bolded box), that are the subject of this guidance.

Figure 1. Relationship of PKI-unique Records



Several additional considerations define the scope of this guidance document:

- PKI records in general do not constitute a unique body of records so basic records management regulations, standards and good practices all apply equally to records created or received in a PKI environment.
- This guidance addresses the need for records management according to the particular mode within which the PKI-unique records are being or will be retained. Guidance is provided for two basic modes:
 - *Operational System:* The need for records management guidance is especially critical for operational systems because little if any guidance exists and operational systems typically do not provide the functionality that is necessary for managing records. Operational systems maintain records in such a way that they can be accessed rapidly in the day-to-day activities of running a PKI, and potentially for a shorter time period than the authorized retention period. Many of the records that are required to establish the validity of a certificate or the operational integrity of the PKI at a given point in time are created or received and maintained on an operational system, such as the system operated by a CA or Registration Authority (RA). Since these records may be the official and possibly the only source of this information during part if not all of the authorized retention period, the operational system can be said to contain the “record file copy”⁶ of that information.
 - *Recordkeeping System:* A recordkeeping system typically does not “create” records, rather it receives electronic records from an operational PKI system or from an office productivity application (e.g., word processing) or tracks paper records, or scanned, digital images of paper records for the purpose of providing retention and disposition management as well as long term retrieval and reproduction of the record file copy for the authorized retention period. Guidance for a recordkeeping system is required in order to allow for operational records to be transferred to a long-term records management environment and for the management of records created or received outside of the operational system.
- Furthermore, records management guidance is considered in the context of the following sources for a record file copy:
 - *Operational system:* A record file copy of a specific record (e.g., a digital certificate) can be derived from relational database tables that have been populated from content submitted or entered via an Internet form or otherwise key-entered by a subscriber or administrative person, as well as automatically generated event log information.
 - *Office productivity application:* Text-based documents that do not require a handwritten signature to be complete could be retained as the record file copy.

⁶ A “record file copy” is the one final and “official” copy that is retained according to a NARA-authorized retention schedule. For example, if the “record file copy” requires signatures and is being retained in paper format, any electronic copy of that record would be deemed for “reference” purposes only and not governed by this guidance.

- *Paper*: Represents the record file copy when received into a PKI activity in paper form (such as documents from an applicant or other entity used for identity proofing) or if handwritten signatures need to be affixed to finalize the document or content, e.g., subscriber agreement, Certificate Policy (CP) or Certification Practice Statement (CPS). The documents may be printed from an operational system (such as from a database form or template) or from an office productivity application in order to apply handwritten signatures.
- *Digital Images*: A paper record also may be scanned and converted to a digital image that is retained and tracked in electronic form.
- This guidance presumes that the implementation, operation and management of a PKI may involve disparate technology platforms and architectures that can change over time. Therefore, the requirements and good practices delineated in this guidance are technology independent.

This guidance is limited to defining and describing the requirements (or “what” is needed) for meeting records management regulations and good recordkeeping practices for PKI-unique administrative records. It does not define nor suggest “how”, i.e., which technology or products should be employed to implement the guidance.

This guidance does not define nor recommend retention schedules, since they are developed to meet the specific needs of each agency’s PKI implementation and then approved by NARA.

The management of records retained by individual subscribers (i.e., protection and maintenance of private key records) is not covered by this guidance.

This guidance is not intended to be a primer or educational tool for understanding cryptography or the technical details of how a PKI functions or operates. Please refer to the Web site of the National Institute of Standards and Technology (NIST) for information related to cryptography and PKI technology in the form of Federal Information Processing Standards and informational NIST publications – <http://csrc.nist.gov/pki/documents/>.

4. PKI Records Producing Functions and Activities

The objective of this section is to present a functional view of a PKI administrative environment where records are created or received and managed.

In the overall context of information resource management systems or information technology, a PKI primarily is a cryptographic security architecture and infrastructure and should be treated as such in the planning, documentation, implementation and management of the PKI. Certain functions and activities of a PKI generate records that may entail unique management requirements. However, there are many activities that merely support a PKI and produce records that are found in other security infrastructures. In this context, the general policies, procedures and requirements defined in Appendix III, Security of Federal Automated Information Resources of OMB Circular No. A-130, should be considered and applied, where applicable, in the management of administrative records produced in conjunction with a PKI.

The major sources used in developing this overview of PKI functions and activities are:

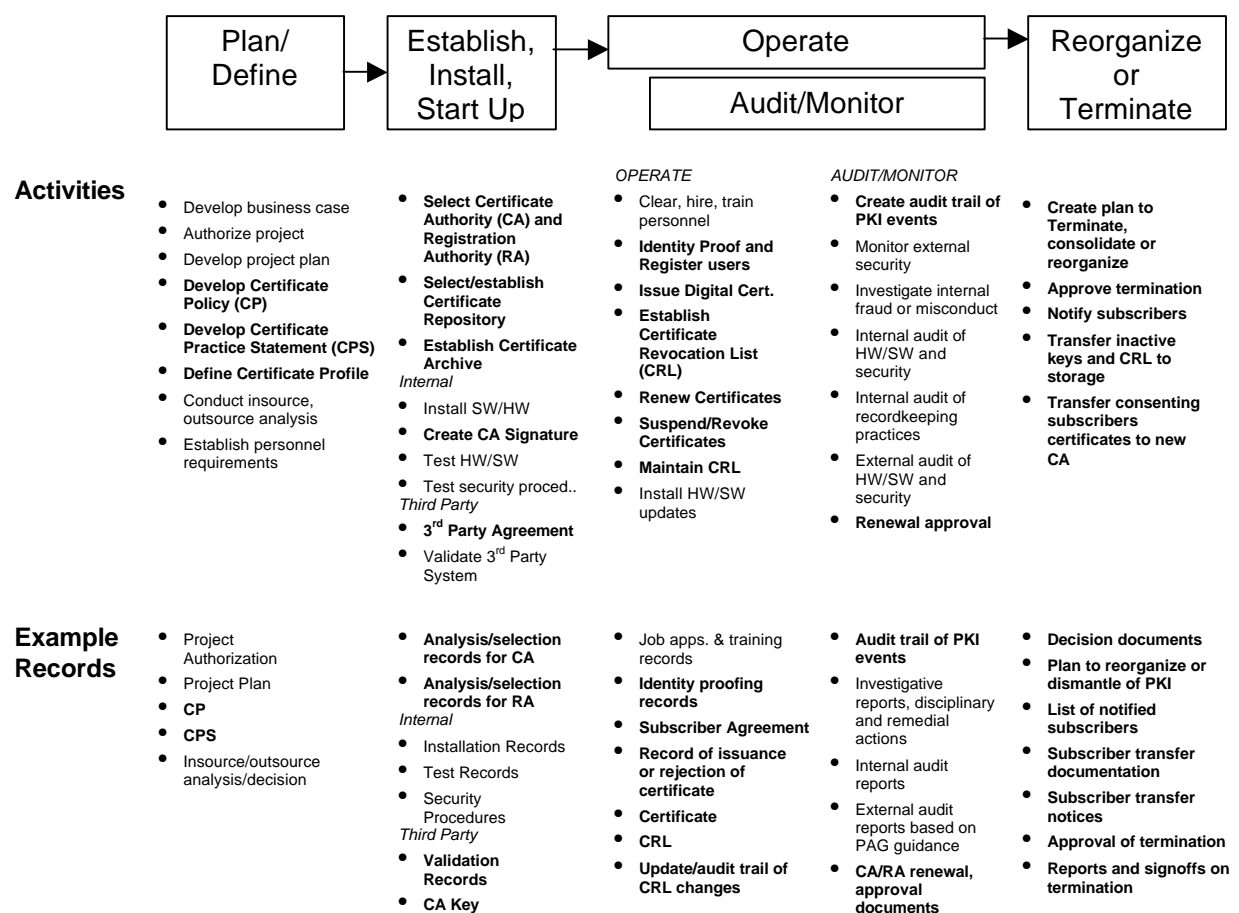
- *Introduction to Public Key Technology and the Federal PKI Infrastructure*, 26 February 2001, National Institute of Standards and Technology
- *Federal Agency Use of Public Key Technology for Digital Signatures and Authentication*, NIST Special Publication 800-25, October 2000, National Institute of Standards and Technology, Federal Public Key Infrastructure Steering Committee, Kathy Lyons-Burke
- *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*, July 2001
- *X.509 Certificate Policy For The Federal Bridge Certification Authority (FBCA)*, October 2001, Version 1.06
- *CARAT Guidelines for Constructing Policies Governing the Use of Identity-Based Public Key Certificates*; National Automated Clearing House Association (NACHA), The Internet Council Certification Authority Rating and Trust (CARAT) Task Force, January 14, 2000
- *PKI Assessment Guidelines (PAG)*, v0.30, Information Security Committee, Section of Science and Technology, American Bar Association, June 18, 2001
- *WebTrust Program for Certification Authorities*, AICPA/CICA, August 25, 2000, Version 1.0
- *Access Certificates for Electronic Services (ACES) Request for Proposal*, General Services Administration, Amendment 00046, August 27, 1999.

The remainder of this section presents an overview of the PKI administrative record processes with examples of activities and related records.

Figure 1 below broadly depicts the administrative functional processes of a PKI and identifies example activities and example records produced from these activities. These examples of activities and records are not intended to be all inclusive, rather only to provide a perspective (see Table 1. for a more comprehensive listing of PKI administrative activities).

Bolded example activities and records represent the PKI-unique activities that are the focus of this guidance.

Figure 2. PKI Administrative Processes – Example Activities and Records



Bolded = PKI-unique Activities & Records

Table 1. PKI Functions/Activities Differentiated As Either PKI-Unique or Supporting, presents a more complete list of example functions and activities of a PKI and differentiates them as being either unique or supporting a PKI environment. However, there may be other activities that are unique to a particular PKI application or to a particular CA's implementation. The records management guidance defined in Section 5 is designed for the PKI-unique activities identified in this table and the activities and records identified in Appendix B. Example PKI-unique Administrative Records Series.

Table 1. PKI Functions/Activities Differentiated As Either PKI-Unique or Supporting

EXAMPLE RECORDS-GENERATING FUNCTIONS/ACTIVITIES	PKI – UNIQUE	PKI SUPPORTING
Plan and Define PKI Environment		
• Develop Business Case and Requirements		X
• Perform Risk/Cost Analysis (determine level vs. cost of security infrastructure)		X
• Authorize Project		X
• Develop Project Plan		X
• Develop Certificate Policy (CP) ⁷	X	
• Develop Certification Practice Statement (CPS) ⁸	X	
• Define Certificate Profile	X	
• Concept of Operations	X	
• Develop PKI SOPs per CP and CPS	X	
• Develop record keeping strategy and procedures per CP and CPS	X	
• Conduct insource/outsource (3 rd party) analysis		X
• Establish Personnel Requirements		X
Establish/Install/Start Up		
• Select CA (internal or third party)	X	
• Select RA (internal or third party)	X	
• Review and approve third party CA, RA CPS (as required)	X	
• Conduct CA/RA accreditation	X	
• Select/Establish Certificate Repository	X	
• Establish Certificate Archive	X	
<i>Internal Install</i>		
• Acquire Software and Hardware		X
• Install Software		X

⁷ The Certificate Policy should delineate the policies for operational and record keeping systems.

⁸ The Certification Practice Statement should state the practices that will be employed to manage PKI-unique records.

EXAMPLE RECORDS-GENERATING FUNCTIONS/ACTIVITIES	PKI – UNIQUE	PKI SUPPORTING
• Install Hardware		X
• Test and validate hardware and software		X
• Test Security Procedures		X
• Create CA Public Key Pair (Key Ceremony)	X	
<i>Third Party Execution</i>		
• Develop/Execute Third Party Contractor Agreement		X
• Develop Contractual Record Keeping Agreement	X	
• Validate 3rd party systems		X
Operate		
• Personnel: clear (background checks), hire, and train		X
• Identity proofing	X	
• Register users	X	
• Issue Digital Certificate (implicitly includes generate keys, deliver public or private key, prove possession of private key and verify public key)	X	
• Establish Certificate Revocation List (CRL)	X	
• Maintain CRL	X	
• Maintain CARL (CA Revocation List – FBCA)	X	
• Renew Certificates	X	
• Revoke/suspend Certificates	X	
• Install HW/SW updates		X
<i>Interoperate (FBCA)</i>		
• CA identity proofing	X	
• Policy mapping	X	
• Technical interoperability testing	X	
• Cross certification agreements	X	
• Border Directory technical specifications	X	
Audit/Monitor		
• Create audit trail data of PKI events, e.g. certificate revocation, certificate renewal, etc.	X	
• Monitor external security		X
• Investigate internal fraud or misconduct		X
• Internal audit of SW and security		X
• Internal audit of records management practices		X
• External audit of HW/SW and security		X
• Cross certification audits	X	
Reorganize or Terminate Operations		

EXAMPLE RECORDS-GENERATING FUNCTIONS/ACTIVITIES	PKI – UNIQUE	PKI SUPPORTING
• Terminate, consolidate or reorganize plan	X	
• Approval	X	
• Notify subscribers	X	
• Transfer inactive keys and CRL to storage	X	
• Transfer consenting subscribers certificates to new CA for reissuance	X	
• Revoke all certificates	X	
• Shutdown and dispose of RA and CA HW/SW		X
• Destroy CA private keys	X	

5. PKI-Unique Records Management Guidance

The PKI-unique records management guidance is segmented into two areas, one for operational systems and one for recordkeeping systems (as identified and previewed in Section 3. Purpose and Scope). Since a record file copy is established as soon as data content or document content is finalized or received, both the operational and recordkeeping systems will have obligations for managing the records during the authorized retention period. However, the operational and recordkeeping systems have fundamentally different purposes and require different approaches for managing records:

- 1) *Guidance for Operational Records*, Section 5.1: In most PKI operational systems, the active content (such as public key certificate data elements) and event information (audit log) typically are stored in relational database tables. While the data may be backed up for disaster recovery purposes, operational systems typically do not provide the necessary functionality to effectively manage records disposition nor other traditional records management functions. For example, a PKI system periodically may create a backup copy of “auditable events,” but only the most recent three or four copies are kept because older copies are overwritten by the newer copies.

Since little if any records management guidance exists for operational systems and they typically do not provide the functionality that is necessary for records management, the need for guidance is especially critical.

In order to emphasize the necessity for implementing records management functionality in operational systems, the guidance for operational systems is intentionally kept separate from that of recordkeeping systems (even though there is some overlap in the individual guidance points).

- 2) *Guidance for Recordkeeping Systems*, Section 5.2: The basis of the guidance for recordkeeping systems is to ensure that all trustworthy PKI-unique records are preserved as evidence for the authorized retention period. Guidance for a recordkeeping system is required for the following reasons:
 - To manage PKI-unique administrative records (and possibly other supporting PKI administrative records) that are not created or received by the operational system, such as paper records and electronic records that are created on office productivity applications or are scanned images of paper documents. The guidance for recordkeeping systems applies to all PKI-unique records independent of the media on which they are stored.
 - To provide for the transfer of operational system records to a recordkeeping system when the status of the record (no longer current or active) or certain events related to one or more records occur (e.g., expiration of a public key certificate).

A key premise for this guidance is that PKI-unique administrative records do not constitute a new category of records that require a total “reinvention” of life cycle records management policies and guidance. While the records a PKI produces may be unique in their content and application, the records management practices, as already embodied in certain federal statutes, regulations, guidance and standards, still apply.

The guidance tables in Sections 5.1 and 5.2 have two columns, Guidance and Source. A source for each guidance is cited and is drawn from the following references:

- OMB A-130 (Appendix 1 and III)
- FBCA X.509 Certificate Policy
- NARA 36 CFR Regulations
- DoD 5015.2 Standard
- ISO 15489, Part 2
- GSA ACES Certificate Policy
- Good practice

Good practice is cited in those instances where no specific regulatory source or other official standard or framework can be cited, yet where the guidance point is very important to ensure proper management of records for the authorized retention period. This is particularly the case in defining certain records management guidance for operational systems and for the transfer of records from an operational to a recordkeeping system. Good practice guidance is derived from various records management studies and reports and from knowledge and experience derived in the process of applying good records management practices in commercial and public entities.

This guidance applies whether the PKI operational system and recordkeeping system are controlled internally by an agency, by a contractor or some mix of the two.

This guidance takes into account the stipulation to avoid “undue or excessive recordkeeping requirements” as mandated by the Paperwork Reduction Act and the CARAT Guidelines.⁹ In other words, this guidance is kept to a minimum with the goal of achieving good records management while allowing federal agencies as well as PKI operational system vendors and recordkeeping system vendors to implement the guidance without undue cost.

⁹ “CARAT Guidelines, Guidelines for Constructing Policies Governing the Use of Identity-Based Public Key Certificates,” (National Automated Clearing house Association – NACHA, January 14, 2000): p. 113.

5.1 Guidance for Operational Systems

The guidance in this section is organized into thirteen separate categories that encompass the PKI-unique activities identified in the operations and audit components of Table 1. PKI Functions/Activities Differentiated As Either PKI-Unique or Supporting.

A key operational systems requirement is to determine whether and when PKI-unique administrative records will be transferred from an operational systems environment to a recordkeeping systems environment. Neither the FBCA X.509 CP nor 36 CFR specifically address this point because in most instances the transfer may depend upon the operational status of the records or the length of the retention period. NARA regulations refer to “current” and “non-current records.” The latter includes records that are no longer required for current agency business.¹⁰ From the perspective of PKI-unique records, one instance of non-current records would be expired digital certificates. Nonetheless, this section presumes that, at some point in time during the authorized retention period, PKI-unique administrative records will be transferred from an operational systems environment to a recordkeeping system environment.

5.1 Guidance for Operational Systems	
Guidance	Source
1. Records Capture	
1.1 Enable the capture, automatically where possible, of accurate and complete records at or near the time of the event	Good Practice
1.2 Support automatic tracking of all activities relating to the capture of records in an event log, including identification of the individual initiating the activity and the time and date	FBCA X.509 CP, 4.51
1.3 Support automatic population of records series title, retention period, and vital records status	DoD 5015.2 ¹¹

¹⁰ NARA regulations do not specifically define when current (active) records become non-current (inactive) records because this is largely seen as a records disposition issue that is determined by the business needs and legal requirements of each agency. The notion of current v. non-current records is rooted in the management of paper records where, after some elapse of time, records that were infrequently accessed could be moved from costly office space to less costly storage areas. There is a parallel with electronic records stored in an operational system where, after a period of time when the records are no longer frequently accessed or when they expire (such as an expired digital certificate), they could be moved to a recordkeeping system for longer term management and access.

¹¹ DoD 5015.2 C2.2.3.10 establishes the precedence for the concept of automatic population of data relevant for record capture.

5.1 Guidance for Operational Systems	
Guidance	Source
<p>2. Record Metadata¹²</p> <p>2.1 The minimum attributes to be captured for each PKI-unique event (both for audit log and event data records, e.g., certificate issuance, CRL entries) to facilitate records management are:</p> <p>For Retrieval:</p> <ul style="list-style-type: none"> - Common Name - Certificate Number - Date of Event - Distinguished Name (when available) <p>For Retention and Business Resumption Management</p> <ul style="list-style-type: none"> - Records Series Title - Records Series Retention Period - Vital records status <p>2.2 Restrict changes in metadata to authorized users</p>	<p>DoD 5015.2¹³</p> <p>DoD 5015.2</p>
<p>3. Records Retrieval</p> <p>3.1 Support searching, retrieving, and rendering of records based upon one or more record attributes (e.g., common name or retention period)</p> <p>3.2 Support the rendering of any retrieved record (e.g., a digital certificate) in a form that is usable by humans</p> <p>3.3 Support browsing and graphical navigation of retrieved records</p>	<p>36 CFR 12234.22</p> <p>36 CFR 1234.24</p> <p>Good Practice</p>
<p>4. Records Disposition</p> <p>4.1 Provide a means to determine the retention status of records using the Record Series and/or Retention period attributes identified in 2.1 and 2.2 above</p>	<p>Good Practice</p>

¹² These metadata attributes are intended to provide a means for managing retention in the operational environment, or to ensure that these critical records management attributes are available should the operational records be transferred at a later date to a recordkeeping environment.

¹³ DoD 5015.2 C2.2.3.2 establishes a precedent of specifying mandatory recordkeeping metadata components.

5.1 Guidance for Operational Systems	
Guidance	Source
4.2 Enable time, event, and time-event dispositions ¹⁴	DoD 5015.2
4.3 Provide a means to delete individual records based on their retention status	Good Practice
4.4 Restrict the capability of defining the record series title and retention period to authorized individuals	Good Practice
4.5 Enable changes in record series titles and retention periods by authorized individuals	Good Practice
4.6 Restrict records destruction commands and instructions to authorized users	FBCA X.509 CP, 4.6.3
4.7 Enable identification of records that have no assigned disposition (e.g., the Records Series Title or Records Retention attributes are missing or null value) including the ability to produce a list of such records	Good Practice
5. Records Integrity	
5.1 Prevent unauthorized access to records	36 CFR 1234.28
5.2 Prevent any changes to stored records – protect the record for as long as it resides in the system	DoD 5015.2
5.3 Ensure that an auditable entry is captured for all events associated with extending the usability of records over time through media renewal or migration	Good Practice
5.4 Prevent modification or deletion to event log entries	FBCA X.509 CP, 4.5.4
5.5 Maintain at least one up-to-date copy of all records and associated metadata off site in the event one or more records is corrupted or otherwise becomes unreadable	36 CFR 1234.28
6. Records Storage (Operational)	
6.1 Prevent unauthorized physical access to records	36 CFR 1234.28

¹⁴ Time disposition occurs when records are immediately available for disposition after the conclusion of a fixed period of time. Event disposition is when records are eligible for disposition immediately after the conclusion of a fixed period of time (e.g., destroy when superseded). Time-event disposition occurs when a retention period is triggered by an event (e.g. transfer digital certificates to a recordkeeping system 60 days after expiration of the certificate).

5.1 Guidance for Operational Systems	
Guidance	Source
6.2 Support the backup of records with a frequency that assures complete recovery	FBCA X.509 CP, 4.6.2
6.3 Maintain duplicate or back-up copies of records in geographically separate repositories from the record copy	36 CFR 1234.30
6.4 Use external labels with removable storage media to provide unique identification for the records, including date of creation	36 CFR 1234.30
6.5 Store records in a stable environment where the temperature and relative humidity are maintained at 62° to 68° Fahrenheit and 35% to 45% Relative Humidity	36 CFR 1234.30
6.6 Implement a comprehensive disaster recovery plan	36 CFR 1234.30
7. Vital Records	
7.1 Identify records that are essential to resumption of business if there is a natural disaster or system failure (see recommendation for including a Vital Record attribute in 2.1 above)	36 C FR 1236.22
7.2 Ensure that vital records can be quickly and fully recovered	36 CFR 1236.24
7.3 Support the authorized destruction of vital records	36 CFR 1236.28
8. Records Audit Trail	
8.1 Ensure that all actions related to records retention and disposition are recorded as auditable events	Good Practice
8.2 For each records retention or disposition event, capture the following attributes as an auditable event log record: <ul style="list-style-type: none"> • Common Name • Distinguished Name (when available) • Certificate Serial Number • A success or failure indicator • Type of actionable event 	FBCA X.509 CP, 4.5.1

5.1 Guidance for Operational Systems	
Guidance	Source
<ul style="list-style-type: none"> • Identity or entity or operator that caused the event • Date and time <p>8.3 Support the transfer of event log records to a recordkeeping system</p>	Good Practice
<p>9. Records Privacy¹⁵</p> <p>9.1 Ensure that physical and electronic security methods protect against unauthorized access to records and associated metadata that are considered private</p> <p>9.2 Protect the privacy of records collected during identity proofing and applicant registration</p> <p>9.3 Support authorized revision or correction of any subscriber record or metadata information that is not correct</p> <p>9.4 Ensure that subscriber records are used only for the purposes for which they were collected</p>	<p>GSA ACES CP, 2.8</p> <p>GSA ACES CP, 2.8</p> <p>GSA ACES CP, 2.8</p> <p>GSA ACES CP, 2.8</p>
<p>10. Records Security</p> <p>10.1 Protect records from unauthorized physical and electronic access</p> <p>10.2 Maintain controlled access to the repository where records are physically stored</p> <p>10.3 Maintain a physical access log that is inspected periodically</p> <p>10.4 Support the use of techniques to detect unauthorized changes in records</p>	<p>FBCA X.509 CP, 4.6.3</p> <p>FBCA X.509 CP, 5.1.2</p> <p>FBCA X.509 CP, 5.1.2</p> <p>Good Practice</p>

¹⁵ GSA ACES CP, Section 2.8 states: "The Authorized CA shall protect the confidentiality of personal information regarding Subscribers that is collected during the applicant registration, ACES Certification application, authentication, and certificate status checking processes in accordance with the Privacy Act of 1974, and Appendix (I and) III to OMB Circular A-130." The Department of Justice is the designated lead agency in the interpretation of Privacy Act requirements.

5.1 Guidance for Operational Systems	
Guidance	Source
11. Record Freezes/Holds	
11.1 Check records against existing hold or freeze orders prior to authorized destruction of records to ensure that they are not inadvertently deleted	36 CFR 1228.54
11.2 Optionally, extract records that have been identified as part of a hold or freeze order from the operational system and move to a recordkeeping system for management during the hold or freeze period	36 CFR 1228.54
11.3 Ensure that only authorized users may implement the guidance identified in 11.1 and 11.2 above	Good Practice
12. Records Transfer to a Recordkeeping System	
12.1 Support transfer of records and associated metadata to an electronic recordkeeping system on fulfillment of specified criteria, that may include: <ul style="list-style-type: none"> • Cut-off date for non-current or non-active records such as the end of a quarter, the calendar year, fiscal year, or other defined cycle • Elapsed time since the occurrence of a specified event such as the expiration of a digital certificate • Cut-off based upon the data base supporting the PKI reaching a certain percentage of total storage capacity 	Good Practice
12.2 Generate an auditable event that documents the date of transfer of records to the recordkeeping system	Good Practice
12.3 Confirm the integrity of transferred records by verifying that no record was altered during their transfer to a recordkeeping system	Good Practice
12.4 All of the documentation and metadata (including the record series title, retention period, and vital records status) associated with the transferred records must be transferred to the recordkeeping system.	Good Practice

5.1 Guidance for Operational Systems	
Guidance	Source
13. Long Term Retention (Operational System)	
13.1 Ensure that records can be retrieved, viewed, reproduced, and processed during the authorized retention period	36 CFR 1234.30
13.2 Adopt a storage medium that has both a life expectancy of at least 20 years and multi-vendor support	Good Practice
13.3 Migrate records from old storage media to new storage media every ten years	36 CFR 1234.30
13.4 Transfer records to an electronic recordkeeping system as appropriate (see 12.1)	36 CFR 1234.24 (c) ¹⁶
13.5 Validate the integrity of electronic records after every preservation activity by confirming that no record has been changed	Good Practice
13.6 Maintain a preservation history file that documents all actions taken to preserve records	Good Practice

¹⁶ This guidance is based upon the precedent of 36 CFR 1234.24 for transferring scheduled e-mail messages from an operational e-mail system to recordkeeping system.

5.2 Guidance for Recordkeeping systems

This guidance is organized into eleven separate categories that encompass the PKI-unique activities identified in all example functions and activities identified in Table 1. PKI Functions/Activities Differentiated As Either PKI-Unique or Supporting.

The guidance for recordkeeping systems provides for the situation whereby records being managed in an operational system that are no longer considered current or active, or for other valid purposes, will be transferred to a recordkeeping system in order to ensure that records are preserved as evidence in a trustworthy and usable manner for the authorized retention period. The recordkeeping system guidance also applies to records that are not created or received by a PKI operational system, such as paper records and electronic records that are created on office productivity applications or are scanned images of paper documents.

This recordkeeping guidance applies to all PKI-unique administrative records independent of the media on which they are stored.

An example of a recordkeeping system is a Records Management Application that has been certified under DoD 5015.2.

5.2 Guidance for Recordkeeping Systems	
Guidance	Source
1. Records Capture 1.1 Receive records from an operational system according to the following guidance: If in the form of database tables: <ul style="list-style-type: none">- Transfer sufficient metadata to support retrieval and retention management- Retain operational system software in which the tables resided during the retention period to enable restoration and rendering for reproduction Records received in “as-rendered-for-viewing” format are to: <ul style="list-style-type: none">- Be in a technology neutral format- Provide metadata sufficient to support retrieval and	36 CFR 1234.24 ¹⁷

¹⁷ *ibid*

5.2 Guidance for Recordkeeping Systems	
Guidance	Source
<p>retention management in the form of a file that can be automatically loaded or manually entered into the recordkeeping system</p> <p>1.2 Accept import of PKI-unique record file copy in technology neutral formats (e.g., XML, RTF) from office productivity systems</p> <p>1.3 Support management of records in paper format, e.g., a CP or CPS that contains handwritten signatures</p> <p>1.4 Maintain an event log that documents the date of transfer from an operational system to a recordkeeping system</p> <p>1.5 Confirm integrity of records by verifying that no changes have occurred in records received from an operational system</p> <p>1.6 Ensure that all of the metadata, supporting event log data, and information associated with a record are completely and accurately transferred</p>	<p>Good Practice</p> <p>36 CFR 1234.22</p> <p>Good Practice</p> <p>Good Practice</p> <p>36 CFR 1234.32</p>
<p>2. Records Metadata</p> <p>2.1 Transfer the minimum attributes specified in the guidance for Operational Systems to the recordkeeping system</p> <p>2.2 For electronic records created in an office productivity system or for paper records or scanned images of paper records, metadata should be captured that is consistent with the minimum requirements stated in Section 5.1.2 Metadata. This is required in order to be able to retrieve all records related to a subscriber (e.g., using common name) or to an auditable event. Metadata in addition to the operational metadata may be required such as for a CP or CPS that cannot be identified with a common name or certificate number. Identification using PKI-unique attributes, such as the associated ObjectID of the record, may be required.</p> <p>2.3 Support the capability to view and print complete record metadata or user-specified portions of the metadata</p>	<p>Good Practice</p> <p>Good Practice</p> <p>DoD 5015.2</p> <p>DoD 5015.2</p>

5.2 Guidance for Recordkeeping Systems	
Guidance	Source
<p>2.4 Support assignment of a unique computer-generated record identifier for each record (electronic or paper) regardless of where the record is stored</p> <p>2.5 Support identification of record location in terms of the hard copy file or electronic location (system, path, and media)</p> <p>2.6 Support generation of a human readable and computer readable bar code label to be attached to all paper records</p> <p>2.7 Restrict changes to records, files, sub-series, and series to authorized individuals</p>	<p>Good Practice</p> <p>DoD 5015.2</p> <p>Good Practice</p>
<p>3. Records Classification</p> <p>3.1 Support a classification scheme that can represent records, files, sub-series, and series organized in a hierarchy with a minimum of four levels.</p> <p>3.2 Logically aggregate individual records into files (folders)</p> <p>3.3 Logically aggregate files into records sub-series</p> <p>3.4 Logically aggregate records sub-series into records series</p> <p>3.5 Support browsing and graphical navigation of the files and classification scheme structure; and the selection, retrieval and display of electronic records and their contents through this mechanism.</p> <p>3.6 Maintain an audit trail of any records, files, sub-series, and series that are reclassified so that their entire history can be reconstructed</p>	<p>DoD. 5015.2</p> <p>36 CFR 1234.24</p> <p>36 CFR 1234.24</p> <p>36 CFR 1234.24</p> <p>Good Practice</p> <p>Good Practice</p>
<p>4. Records Retrieval</p> <p>4.1 Support retrieval and viewing or reproduction of records based upon one or more metadata attributes (e.g. common name, date-range, records series, etc)</p> <p>4.2 Support retrieval, and rendering of a specific PKI-unique record (e.g., digital certificate or multiple digital certificates</p> <p>4.3 Support the rendering of any retrieved record (e.g., a digital certificate) in a form that is usable by humans</p>	<p>DoD 5015.2</p> <p>Good Practice</p> <p>36 CFR 1234.24</p>

5.2 Guidance for Recordkeeping Systems	
Guidance	Source
4.4 Restrict retrieval of records based upon user access permissions	Good Practice
4.5 Support browsing and graphical navigation of retrieved records	DoD 5015.2
5. Records Disposition	
5.1 Restrict the capability for defining retention periods, disposition actions, and the changing of retention periods to authorized individuals	DoD 5015.2
5.2 Enable time, event, and time-event disposition	
5.3 Enable automatic calculation of destruction date where appropriate	DoD 5015.2 DoD 5015.2
5.4 Support authorized changes in the disposition of records, files, records sub-series, and records series	DoD 5015.2
5.5 Support authorized individuals to enter data indicating when a specified event or time-event has occurred that affects the authorized retention of records	DoD 5015.2
5.6 Support authorized individuals to view the disposition attributes for each record, file, record sub-series, or records series	Good Practice
5.7 Support the identification and rendering of records, including associated metadata, that are eligible for destruction	DoD 5015.2
5.8 Support the requirement for a second confirmation from an authorized user before deleting records	DoD 5015.2
5.9 Produce documentation related to all authorized record destruction	DoD 5015.2
6. Records Integrity	
6.1 Prevent unauthorized access to records	36 CFR 1234.28

5.2 Guidance for Recordkeeping Systems	
Guidance	Source
<p>6.2 Prevent any changes to stored records – protect the record for as long as it resides in the system</p> <p>6.3 Prevent modification or deletion to records history log entries</p> <p>6.4 Maintain a second up-to-date copy of all records and associated metadata, including history log entries, off site for records recovery</p>	<p>DoD 5015.2</p> <p>FBCA X.509 CP 4.5.4</p> <p>36 CFR 1234.30</p>
<p>7. Records History Log</p> <p>7.1 Ensure that all activities taken to ensure the continued usability of records through media renewal or migration to a new technology platform are fully documented in a records history log</p>	<p>Good Practice</p>
<p>8. Records Privacy¹⁸</p> <p>8.1 Physical and electronic security methods must protect against unauthorized access to records and associated metadata that are considered private</p> <p>8.2 Protect the privacy of records collected during identity proofing and applicant registration</p> <p>8.3 Support authorized revision or correction of any subscriber record or metadata information that is not correct</p> <p>8.4 Ensure that subscriber records are used only for the purposes for which they were collected</p>	<p>GSA ACES CP, 2.8</p> <p>GSA ACES CP, 2.8</p> <p>GSA ACES CP, 2.8</p> <p>GSA ACES CP, 2.8</p>
<p>9. Records Security</p> <p>9.1 Protect records from unauthorized deletion</p> <p>9.2 Maintain controlled access to the repository where records are stored</p> <p>9.3 Maintain an access log that is inspected periodically</p> <p>9.4 Block external access to records through an electronic</p>	<p>36 CFR 1234.28</p> <p>FBCA X.509 CP, 5.1.2</p> <p>FBCA X.509 CP, 5.1.2</p> <p>Good Practice</p>

¹⁸ See footnote 15

5.2 Guidance for Recordkeeping Systems	
Guidance	Source
<p>“firewall”</p> <p>9.5 Use techniques to detect unauthorized changes or modifications to electronic records</p> <p>9.6 Store duplicate or back-up copies of records in a geographically different archives or recordkeeping storage facility</p> <p>9.7 Implement a comprehensive disaster recovery plan</p>	<p>Good Practice</p> <p>36 CFR 1234</p> <p>36 CFR 1236.26</p>
<p>10. Record Freezes/Holds</p> <p>10.1 Provide the capability for authorized individuals to identify records that are subject to a “hold” or “freeze” order</p> <p>10.2 Provide the capability to extend or suspend (freeze/hold) the retention period of records beyond their scheduled disposition</p> <p>10.3 Provide the capability for authorized individuals to “unfreeze” records</p>	<p>36 CFR 1228.54</p> <p>36 CFR 1228.54</p> <p>36 CFR 1228.54</p>
<p>11. Records Preservation</p> <p>11.1 Retain PKI software and hardware necessary to read, search, retrieve, and render records</p> <p style="text-align: center;">OR</p> <p>11.2 Support the capability to ensure the usability and trustworthiness of records throughout their authorized retention through migration to new software recordkeeping system applications, new storage media, or new vendor technology neutral formats</p> <p>11.3 Prevent unauthorized physical/electronic access to the facility the records are stored</p> <p>11.4 Adopt a storage medium that has a predicted life expectancy of at least 20 years and has multi-vendor support</p> <p>11.5 Renew storage media through copying (exact duplication of the bit stream) or reformatting records from old storage</p>	<p>FBCA X.509 CP 4.62</p> <p>DoD 5015.2</p> <p>36 CFR 1234.28</p> <p>Good Practice</p> <p>36 CFR 1234.30</p>

5.2 Guidance for Recordkeeping Systems	
Guidance	Source
media to new storage media (e.g., 3480 tape to 3490 tape) every ten years	
11.6 Confirm after each media renewal activity (e.g., copy) that no record has changed	Good Practice
11.7 Migrate records to a technology neutral file format (e.g., XML, RTF) that has substantial vendor support	Good Practice
11.8 Store records in a stable environment where the temperature and humidity are maintained at 62°to 72° Fahrenheit and 35% to 45% Relative Humidity	36 CFR 1234.30
11.9 Annually inspect a statistical sample of records in the storage facility to confirm that no catastrophic loss has occurred or may be impending	36 CFR 1234.30
11.10 Create and maintain a preservation history log that documents all actions taken to extend the usability of storage media	Good Practice

Appendix A. Glossary, Acronyms and Abbreviations

Definitions

These definitions are derived from a variety of sources, including the NARA E-Sign guidance, DoD 5015.2, X.509 PKIX, X.509 Certificate Policy for the Federal Bridge Certification Authority (FBCA), and glossaries in several books relating to PKI and digital signatures.

Administrative PKI Record. PKI records that are created, used, maintained, and preserved to support on-going management and operation. They do not include subscriber transactions where a public key has been used for signing or for another purpose

As-rendered-for-viewing record. A Logical PKI Record (see definition) that has been rendered in a human readable, reproducible format, and then saved in that format as the record file copy. For example, a single event, such as a certificate revocation, would be rendered as viewable and usable by inserting the appropriate data elements into a database form or template, then reproduced in a format that could be preserved as the record file copy (such as on paper or in XML format)

Archives. A physical or logical space independent of a production environment where records are protected from loss, alteration, and deterioration so that they may be used as trustworthy evidence for as far into the future as is necessary.

Certification Authority. A trusted organization that either accepts certificate applications from subscribers, issues digital certificates, and maintains status information about certificates or arranges for a trust third party to perform these services.

Certificate Policy. A written document that identifies the applicability of a class of certificates with common security requirements and sets forth the requirements that are appropriate for applications or uses. PKIX has created an outline and guidance for the content of certificate policy documents.

Certification Practice Statement. A written document that articulates the practices that a Certification Authority employs in issuing, managing, revoking, and renewing certificates. PKIX has created an outline and guidance for the content of certificate practice statements.

Certificate Revocation List. This is a Certificate Authority's listing of invalid certificates, due to time lapse, employment change, theft of private key, or other reasons.

Classification. The systematic identification and arrangement of business activities and/or *records* into categories according to logically structured conventions, methods, and procedural

rules represented in a classification scheme. A PKI classification scheme could be designed that defined records, record files or folders, records sub-series, and records series for each of the primary PKI administrative functions.

Common Name. The given name of an individual or organization that corresponds to its real world identity.

Content. The information that a record is meant to convey that may consist of words, phrases, numbers, symbols, and so on.

Context. The organizational, functional, and operational circumstances in which documents are created and/or received and used. The placement of records within a larger records classification system providing cross-references to other related records.

Current Records. Records that are necessary to conduct the current business of an office and therefore are readily available for consultation and reference.

Cut off. Breaking, or ending, files at regular intervals, usually at the close of a fiscal or calendar year, to permit their disposal or transfer in complete blocks or segments.

Disposition. Actions taken regarding records after they are no longer required to conduct current Agency business. (See Non-current record)

Distinguished Name. A unique name or character string for each individual in a CA directory that unambiguously identifies each subscriber.

Emergency Operating Records. (See **Vital Records**)

Event Disposition. A disposition instruction in which a record is eligible for the specified disposition (transfer or destroy) upon or immediately after the specified event occurs. No retention is applied and there is no fixed waiting period as with the "timed" or combination "time-event" dispositions. An example of event disposition would be "Destroy when no longer needed for current operations".

Freeze. The suspension or extension of the disposition of temporary records that cannot be destroyed on schedule because of special circumstances, such as a court order or an investigation, that requires a temporary extension of the approved retention period.

Good Practice. Good practice indicates that no specific regulatory or other official standard or framework can be cited, yet where the guidance point is very important to ensure proper management of records for the authorized retention period. The good practice guidance cited in this document is derived from various records management studies and reports and from knowledge and experience derived from the application of records management practices in commercial and public entities.

Integrity. The integrity of a record refers to its being complete and unaltered over time.

Logical PKI Record. A logical PKI record consists of data content stored in relational database tables that exists only as a physical record at the time of rendering for viewing, printing, or saving. If the rendered physical record is not printed or saved then it ceases to exist as a physical entity. If the data content has not changed then a specific logical record can be retrieved and accurately rendered innumerable times. As an example, the data content of a digital certificate exists physically in two or more relational database tables but the digital certificate exists as a physical entity only at the time that the data content is retrieved and used to populate a digital certificate template. This digital certificate may be printed or saved as a physical entity.

Metadata. Data describing stored data, that is, data describing the structure, content, and context, and other characteristics of electronic records. Record profile data.

Non-current Record. Records that are no longer required to conduct agency business and therefore are ready for final disposition. (See also Current Record)

Object ID. A unique identifier for a Certificate Policy that is registered with the American National Standards Institute so that a certificate issuer and a certificate users (subscriber) can both recognize and reference the policy.

Office Productivity Applications. Software packages that perform a variety of office support functions, such as word processing, desktop publishing, spreadsheet calculations, electronic mail, facsimile transmission and receipt, document imaging, optical character recognition (OCR), work flow, and data management. These applications are generally those used to generate, convert, transmit, or receive business documents.

Operational System. The software and hardware system that performs the day-to-day activities of running and maintaining a PKI, such as a CA. In an operational system, the active content (such as public key certificate data elements) and event information (audit log) typically are stored in relational database tables. Since this content or event data may be the official and possibly the only source of this information for a period of time, the operational system can be said to contain the “record file copy” of that information. While the data may be backed up for disaster recovery purposes, operational systems typically do not provide the functionality that is necessary to effectively manage records disposition nor other traditional records management functions.

Record File Copy. The final and “official” copy that is retained according to a NARA-authorized retention schedule. For example, if the “record file copy” required handwritten signatures and is, therefore, being retained in paper format, any electronic copy of that record would be deemed for “reference” purposes only and disposable at the convenience of the agency.

Recordkeeping System. A manual or automated system in which records are collected, organized, and categorized to facilitate their preservation, retrieval, use, and disposition for the authorized retention period.

Record Series File units or documents arranged in accordance with a filing system or maintained as a unit because they result from the same accumulation or filing process, the same function, or the same activity; have a particular form; or because of some other relationship arising out of their creation, receipt, or use.

Registration Authority. An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e., a Registration Authority is delegated certain tasks on behalf of an authorized CA).

Retention Period. The length of time that records must be kept before they are destroyed. Records not authorized for destruction have a retention period of “permanent.” A retention period is sometimes referred to as “Authorized Retention” because the National Archives has approved the disposition of the records.

Structure. The physical and logical format of a record and the relationships between the data elements

Technology Neutral Format. An openly published file format that supports data interchange and interoperability across heterogeneous product lines, media, devices, and systems.

Time Disposition. A disposition instruction that specifies when a record shall be cut off and when the fixed retention period is applied. The retention period does not begin until after the records have been cut off. Example: "Destroy after two years – cut off at the end of the calendar (or fiscal) year; hold for two years; then destroy".

Time-Event Disposition. A disposition instruction that specifies that a record shall be disposed of a fixed period of time after a predictable or specified event. Once the specified event has occurred, then the retention period is applied. Example: "Destroy three years after close of case".

Vital Records. Essential records that are needed to meet operational responsibilities under national security emergencies or other emergency or disaster conditions (emergency operating records) or to protect the legal and financial rights of the Government and those affected by Government activities (legal and financial rights records). Emergency operating records are the type of vital records essential to the continued functioning or reconstitution of an organization during and after an emergency.

Acronyms and Abbreviations

ACES. Access Certificates for Electronic Services (General Services Administration)

CA. Certification Authority

CARAT. Internet Council Certification Authority Rating and Trust (CARAT) Task Force

CFR. Code of Federal Regulations

CMM. Capability Maturity Model

CP. Certificate Policy

CPS. Certification Practice Statement

CRL. Certificate Revocation List

ERM. Electronic Records Management

FPKISC. Federal Public Key Infrastructure Steering Committee

FBCA. Federal Bridge Certification Authority

L/P WG. Legal and Policy Working Group of the Federal Public Key Infrastructure Steering Committee

OID. Object Identifier

PAG. PKI Assessment Guidelines (American Bar Association)

PKIX. Public Key Infrastructure (X.509) (Internet Engineering Task Force Working Group)

RA. Registration Authority

Appendix B. Example PKI-unique Administrative Records Series

Series 1: Define and Establish A Public Key Infrastructure	
PKI-UNIQUE	
EXAMPLE ACTIVITIES	EXAMPLE PKI-UNIQUE RECORDS BY ACTIVITY
1.1 Determine that a PKI is to be established and create a project implementation plan	1.1 Authorizing documentation and project implementation plan
1.2 Designate the entity to serve as Certification Authority (CA)	1.2 Decision approval records, selection criteria, assessment of available CAs
1.3 Create Certificate Policy (CP), Certification Practice Statement(CPS), and other key operating documents	1.3 Approval of Certificate policy and Certification Practice Statement, and key operating documents
1.4 Develop operating procedures in accordance with Certificate Policy and Certificate Practice Statement	1.4 Operating procedures manual
1.5 Conduct a risk cost analysis as required by GPEA and OMB Implementation Guidelines	1.5 Risk analysis studies, recommendations, guidelines, implementation procedures
1.6 Develop records management policy, including migration strategy for records retained for a long time	1.6 Records management policy, plans, and migration strategies to be implemented
1.7 Select the entity to serve as Registration Authority (RA)	1.7 Decision approval records, selection criteria, assessment of existing RAs
PKI-SUPPORTING	
EXAMPLE ACTIVITIES	EXAMPLE PKI-SUPPORTING RECORDS BY ACTIVITY
1.8 Establish personnel requirements	1.8 Job descriptions, training requirements, background checks

Series 2: Launch/Install A Public Key Infrastructure	
PKI-UNIQUE	
EXAMPLE ACTIVITIES	EXAMPLE PKI-UNIQUE RECORDS BY ACTIVITY
2.1 Install and validate Certification Authority hardware and software	2.1 Installation records, testing procedures
2.2 Install and validate Registration Authority hardware and software	2.2 Installation Record, testing procedures
2.3 Obtain final approval from oversight or authorizing body	2.3 Approval/rejection documents
2.4 Create CA signature key	2.4 Signature key creation record and signature key use/ validity requirements
PKI-SUPPORTING	
EXAMPLE ACTIVITIES	EXAMPLE PKI-SUPPORTING RECORDS BY ACTIVITY
2.5 Test security procedures	2.5 Test results and sample certificates
2.6 Validate certification revocation procedure	2.6 Procedures to follow in revoking certificates and maintenance of a certification revocation list
2.7 Establish backup and storage	2.7 Overall storage policies and practices, including backup procedures and data restoration

Series 3: Operate a Public Key Infrastructure	
PKI-UNIQUE	
EXAMPLE ACTIVITIES	EXAMPLE PKI-UNIQUE RECORDS BY ACTIVITY
3.1 Certification Application	3.1 Verification of identity, identity documentation
3.2 Certificate Issuance and Key Generation	3.2 Notification of applicant and transmitting the certificate to the subscriber or transmitting a protocol to a subscriber that permits local generation of a key pair
3.3 Certificate Acceptance	3.3 Subscriber acknowledgement of acceptance of conditions of use of the certificate, including subscriber obligations
3.4 Certificate Validation	3.4 Identity of requester, identity of certificate, verification or denial, Online Certificate Status Protocol, reason for denial, time/date stamp
3.5 Certificate Revocation	3.5 Confirmation that conditions that merit revocation have been met, Certificate Revocation List , update frequency, individual performing update
3.6 Certificate Suspension	3.6 Confirmation that conditions that merit certificate suspension have been met. Reasons for the suspension, individual performing update
3.7 Certificate Replacement	3.7 Confirmation that conditions which merit certificate replacement have been met and subscriber acknowledgement of receipt of certificate replacement
3.8 Certificate Renewal	3.8 Confirmation that the subscriber has met the CP/CPS conditions for renewal as well as subscriber authorization to renew a certificate that has not been revoked, suspended, or expired
3.9 Create and maintain an event log	3.9 Auditable events specified in FBCA X.509 Certificate Policy

Series 3: Operate a Public Key Infrastructure	
PKI-SUPPORTING	
EXAMPLE ACTIVITIES	EXAMPLE PKI-SUPPORTING RECORDS BY ACTIVITY
3.10 Hire and train personnel	3.10 Job applications, training records, background checks
3.11 Install and validate software updates	3.11 Decision documents, installation and test records
3.12 Notify users of new software	3.12 Notification to affected users, contingency plan if new software does not replicate the functionality of old software

Series 4: Audit and Monitor a Public Key Infrastructure	
PKI-UNIQUE	
EXAMPLE ACTIVITIES	EXAMPLE PKI-UNIQUE RECORDS BY ACTIVITY
4.1.1 Periodic internal review of auditable events specified in X.509 ACES Policy	4.1.1 Audit report, reports on compliance/non-compliance, remedial actions
4.1.2 External review of auditable events specified in X.509 ACES Policy	4.1.2 Audit report, reports on compliance/non-compliance, remedial actions
4.1.3 Monitor compliance with security requirements specified in the CPS and other operating procedures	4.1.3 Reports on compliance audits, remedial actions
PKI-SUPPORTING	
EXAMPLE ACTIVITIES	EXAMPLE PKI-SUPPORTING RECORDS BY ACTIVITY
4.2.1 Investigate internal fraud or misconduct	4.2.1 Investigation reports, disciplinary actions, remedial actions taken
4.2.2 Internal audit of software and systems security	4.2.2 Audit report, reports on compliance with recommendations

	in audit report
4.2.3 External audit of software and system security	4.2.3 Audit reports based upon PAG guidance, reports on compliance with recommendations in audit report

Series 5: Terminate/Consolidate/Reorganize A Public Key Infrastructure	
PKI-UNIQUE	
EXAMPLE ACTIVITIES	EXAMPLE PKI-UNIQUE RECORDS BY ACTIVITY
5.1 Determine that PKI is to be terminate, consolidate, or reorganized	5.1 Studies, reports, recommendation, and action documents
5.2 Obtain approval (if required) from appropriate entities to terminate, consolidate, or reorganize	5.2 Decision documents
5.3 Notify subscribers	5.3 List of individuals/organizations to whom notice has been given, several examples of notices, identification of new CA, and option for subscribers to elect or reject the CA
5.4 Transfer inactive keys and revocation certificate list to storage repository	5.4 Transfer document attesting to legal custody along with access rights
5.5 Transfer consenting subscribers' certificates and related material to new Certificate Authority	5.5 Transfer notices, list of subscribers who have agreed to use the new Certificate Authority
5.6 Destroy sensitive records involving privacy	5.6 Approved disposal of records in accordance with an authorized records schedule
5.7 Shutdown and disposal of RA hardware and CA software	5.7 Shutdown report with signoffs from appropriate individuals

Appendix C. Focus Group Issues

This appendix documents the issues raised during the PKI records management Focus Groups held on 3/18/02 and 3/20/02, as edited and consolidated by Mark Giguere. The response to each issue relative to how it was addressed in the PKI-unique administrative records guidance is presented in *italics*.

Focus Group Session: 3/18/02

1. (NS¹⁹) Segregating out technology-specific (e.g., Baltimore v. Entrust) documentation records.

Vendor documentation, even if technology-specific, is generally considered to be records that are present in every information technology application and, therefore, also would be considered as supporting records in a PKI environment. Since the guidance addresses only PKI-unique records, technology specific or vendor documentation is not specifically addressed in the guidance or the example records series.

2. (NS) Further specification of CRL process management records.

Further specification of CRL (certificate revocation list) activities and example records are covered in the Section 4. Table 1, and in Appendix B, Example PKI-unique Administrative Records Series (FBCA X.509 CP, Section 4.4.3.1 is the primary source for the further specification)

3. (NS) Documentation requirements for the registration authority process.

Activities and example records associated with the registration authority (RA) process are covered in the Section 4. Table 1, and in Appendix B, Example PKI-unique Administrative Records Series (FBCA X.509 CP, Section 3 is the primary source for the activities and examples of the RA).

4. Discuss the implications of maintaining PKI admin.(istrative) records vis-à-vis Privacy Act system requirements/violations.

Records privacy is addressed in the guidance, Section 5.1 Guidance for Operational Systems, Point 9. Records Privacy. The source for the guidance is the GSA ACES CP, Section 2.8.

¹⁹ (NS) identifies a potential a new record series for consideration

FBCA X.509 CP, Section 2.8 states that “FBCA information not requiring protection shall be made publicly available.” More to the point is a detailed discussion of confidentiality in Certificate Policy for Access Certificates for Electronic Services (ACES), Section 2.8.

5. Contractor maintenance of PKI records

In general, contractor maintenance of records, including PKI records, is covered by a General Records Schedule. However, when a contractor produces PKI-unique administrative records, the contractor agreement should state that they will comply with the PKI-unique guidance delineated in Section 5. and, of course, NARA General Records Schedules, regulations, and guidance on electronic signatures.

6. Identify retention requirements for PKI records specified in other laws.

Retention requirements are not addressed as part of the guidance because retention periods for new records series, such as PKI-unique records, are authorized on an individual basis by NARA. As a general rule, most statutes do not specify retention requirements and, if they did, they would not automatically or necessarily apply to or have a direct influence on the retention periods for PKI-unique records.

7. Discuss relationship of A-130 ERM requirements for PKI ERM requirements.

The requirements of OMB Circular A-130, Section I and Section III apply in general to the management of a PKI operational application, which is so stated in the introduction to Section 4. PKI Records Producing Functions and Activities.

8. (NS) Specification of CMM related documentation.

Capability Maturity Model (CMM) related documentation is general documentation related to every information technology application and, thereby, would be considered as PKI-supporting records. While CMM methods could be used to determine the timing or need to upgrade to or transfer records to another technology or a different operational or recordkeeping system, the records resulting from this process would not be considered PKI-unique. Given this assumption, CMM documentation is not specifically addressed, either in the guidance or example records series.

9. Supply model schedules

Since records schedules, as authorized by NARA, are considered on an individual basis for each agency and each information management application, a “model” records schedule cannot realistically be produced. Appendix B. Example PKI-unique Administrative Records Series provides one illustration of what a PKI-unique records schedule may include.

10. Discuss how to integrate PKI PMO (Program Management Office) into RM (Records Management) PMO operations

The proposed First Draft makes a clear distinction between the guidance for a PKI operational system and guidance for a recordkeeping system. The guidance does acknowledge that certain record attributes and metadata should be captured in an operational system that would be transferred to a recordkeeping system. See Section 5.1-2.1, Records Metadata, and 5.2-2.1 and 2.2.

11. (NS) Documentation requirements for private key generation/protection.

Records retention requirements for private key generation and protection should be spelled out in the subscriber agreement, which is identified as a PKI-unique record and would be subject to all PKI-unique guidance stated herein. The records management requirements for any record file copy retained by an individual subscriber are not addressed by this guidance.

12. Need to comport PKI ERM schedules with retention specifications in CPS.

Retention specifications are not addressed as part of the guidance because retention periods for new records series, such as PKI-unique records, are authorized on an individual basis by NARA. While the retention periods specified in the CP or CPS should be considered as overall guidance for determining retention periods, a separate records schedule for each PKI application must be submitted by the agency to NARA for review and authorization.

Focus Group Session: 3/20/02

1. Privacy Act system of records inclusive in PKI administrative records

See issue 4. above from the Focus Group Session of 3/18/02. PKI records meet the criteria for a system of records based on the Privacy Act of 1975.

Records privacy is addressed in the guidance, Section 5.1 Guidance for Operational Systems, Point 9. Records Privacy. The source for the guidance is the GSA ACES CP, Section 2.8.

Also see the GSA Privacy Notification on this point in the Federal Register, May 28, 1999 (Vol. 64, Number 103, 29032-29034).

2. Clear and simple series definitions

The definitions provided in Appendix A., and the overview of PKI functions and activities provided in Section 4. PKI Records Producing Functions and Activities are aimed at addressing this issue.

3. Logical, defensible retention period.

See issues 6., 9., and 12. above from the Focus Group Session of 3/18/02.

Retention specifications are not addressed as part of the guidance because retention periods for new records series, such as PKI-unique records, are authorized on an individual basis by NARA.

4. Preserving integrity of digital signatures across software migrations.

The scope of this guidance does not include guidance for the actual application or use of digital signatures.

However, in the context of preserving the integrity of administrative records underlying the digital signature (such as identity proofing information, the public key certificate and events related to the CRL), guidance is provided in Section 5. Also, specific guidance is provided in Section 5.1, Point 13. and Section 5.2, Point 11. regarding long term preservation, including migration to new software or technology.

5. How to establish linkages between related records (across series and generations of PKI technology)?

One purpose of the metadata guidance identified in Section 5.1, guidance point 2. is to define common relationships among PKI-unique records, such as common name, and records series.

6. Contractor responsibilities vis a vis PKI admin records

See issue 5. above from the Focus Group Session of 3/18/02.

In general, contractor maintenance of records, including PKI records, is covered by a General Records Schedule. However, when a contractor produces PKI-unique administrative records, the contractor agreement should state that they will comply with the PKI-unique guidance delineated in Section 5. and, of course, NARA General Records Schedules, regulations, and guidance on electronic signatures.

7. Why is/isn't this (i.e., PKI ERM) the same as any other ERM?

This issue is addressed by separating the guidance into two distinct areas, one for "operational systems" and another for "recordkeeping systems." The guidance makes the case that PKI records management is not the same as any other electronic records management system, primarily because many key records (such as the data content that makes up the public key certificate and the event records related to the CRL and other administrative events) are maintained in an operational system rather than a recordkeeping system. The records management or "records archival" requirements of an operational system, as typically defined in the respective CP and CPS, do not adequately address the longer term retention of records.

8. How to address FOIA and discovery of PKI ERM records.

Guidance points 9.1-9 in Section 5.1 spell out the basic requirements that must be satisfied with regard to protection of privacy in an operational system. The FBCA X.509 CP and the ACES CP articulate the activities that are necessary to be compliant with FOIA and Privacy.